Index Number | | | | | | | |

1. (a). Describe the primary motivation for implementing a firewall within an organisational network infrastructure.

[5 marks]

[internet is a major requirement for an organisation. But allowing the outside world to reach and interact with the local network assets is a threat to the organisation. A firewall can be inserted between the premises network and the internet to establish a controlled link and establish an outer security wall or perimeter. (Topic 5.4)].

(b). Firewalls employ various techniques to regulate network access. Given that service control is one such method, list down three (3) other distinct techniques used by firewalls for access control.

[3 marks]

[Direction control, User control, Behaviour control, (Topic 5.5)]

(c). Explain the mechanism by which firewalls implement access control using the service control technique.

[5 marks]

[Determines the types of Internet services that can be accessed, inbound or outbound. The firewall may filter traffic on the basis of IP address, protocol, or port number; may provide proxy software that receives and interprets each service request before passing it on; or may host the server software itself, such as a Web or mail service (Topic 5.5/ Chapter 23 reference book)]

Index Number | | | | | | | |

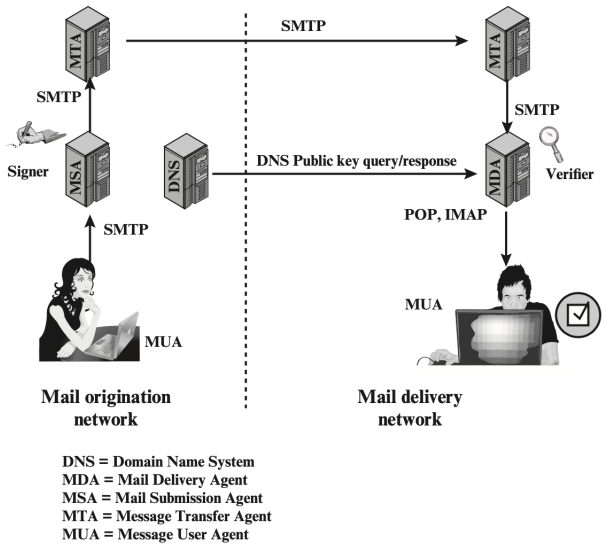
(d). Identify and briefly list four (4) distinct types of firewalls commonly employed in network security.

[4 marks]

[Packet Filtering Firewall, Stateful Inspection Firewalls, Application-Level Gateway, Circuit-Level Gateway]

(e). Provide a detailed illustration, in the form of a diagram, outlining the DomainKeys Identified Mail (DKIM) signing and verification process. The diagram should clearly depict all essential components involved in this email authentication mechanism and their interactions.

[8 marks]



[Topic 6.2.4, Page 651 Reference book]

Index Number | | | | | | | |

2. (a). Describe the characteristics of an ad hoc network and explain the primary security challenges inherent in such network configurations.

[4 marks]

[These are peer-to-peer networks between wireless computers with no access point between them. Such networks can pose a security threat due to a lack of a central point of control. Topic 7.1 - Page 583 reference book]

(b). Write down three (3) methods of securing wireless networks.

[6 marks]

[Use encryption, Use antivirus and antispyware software, and a firewall, Turn off identifier broadcasting, Change the identifier on your router from the default, Change your router's pre-set password for administration, Allow only specific computers to access your wireless network(MAC address filtering) Topic 7.1, Page 585 Reference book]

(c). Explain the inherent security risks associated with utilising untrusted network environments.

[6 marks]

[potentially susceptible to eavesdropping or man-in-the-middle types of attacks. Topic 7.2. Page 587 Reference book]

(d). Maintaining compliance requires a well-defined, systematic approach that integrates both processes and technology. Briefly describe two (02) essential components that should be included in the approach to maintain compliance.

[5 marks]

[Regular assessment of selected security controls,Configuration and control management processes, Change management processes, Annual audit of the security environment. Topic 10.1.3, Ref 2: Pg. (75-79)]

Index Number | | | | | | | |

(e). List down four (4) components of a typical IT infrastructure.

[4 marks]

[User Domain, Workstation Domain, LAN Domain, LAN-to-WAN Domain, WAN Domain, Remote Access Domain, System Application Domain. Topic 10.1.2]

3. (a). Transport Layer Security (TLS) is a combination of protocols working together to secure information communication.

i. What is the Phase III of Handshake Protocol in TLS?

[2 marks]

ANSWER:
Client authentication and key exchange [TLS note slide 21]

ii. Explain the main steps of the Phase III of TLS protocol.

[6 marks]

ANSWER: If the server has requested a certificate, the client begins this phase by sending a certificate message Next is the client_key_exchange message, which must be sent in this phase. The content of the message depends on the type of key exchange. Finally, in this phase, the client may send a certificate_verify message to provide explicit verification of a client certificate [TLS note slide 32]

Index Number | | | | | | | |

(b). Describe the steps involved in a replay attack on an information system and explain two (2) methods that you can use to prevent or reduce the possibility of such attacks.

[8 marks]

The simplest replay attack is one in which the opponent simply copies a message and replays it later

Another attack involves a backward replay without modification. This is a re-play back to the message sender.

Replay attacks can be prevented or reduce the affect of it by using Timestamps and Challenge/response.
[User Authentication slide 10, 11]

(c). Describe Federated Identity using an example.

[5 marks]

Federated identity management refers to the agreements, standards, and technologies that enable the portability of identities, identity attributes, and entitlements across multiple enterprises and numerous applications and supporting many thousands, even millions, of users
[User Authentication slide 35]

Index Number | | | | | | | |

(d). A framework offers IT organizations a method for establishing an approach to managing IT risks. COBIT5 is such a framework. Write the five COBIT5 principles.

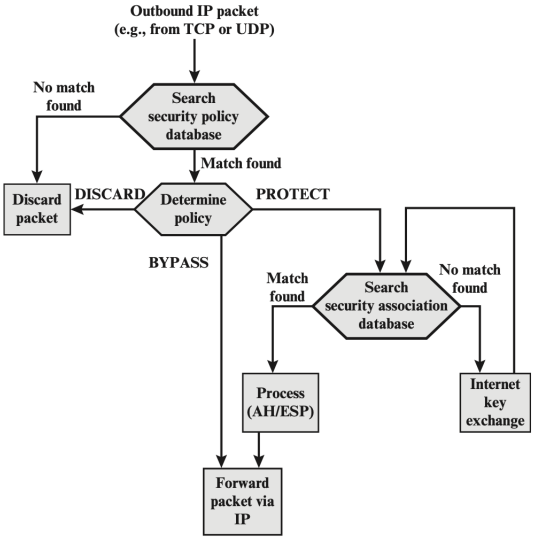
[4 marks]

Meeting stakeholder needs, Covering the Enterprise End to End, Applying a single integrated framework, Enabling a holistic approach, Separating governance from management.
[Ref 2: page 91]

4. (a). Use a diagram to explain the flow of processing a packet in the network layer of IP Security implementation.

[8 marks]

ANSWER:



[Virtual Private Networks slide 28]

Index Number | | | | | | | |

(b). In IP Security, what is the purpose of Security Parameter Index (SPI)?

[3 marks]

ANSWER: To identify a security association [Virtual Private Networks slide 24]

(c). Describe the technique used by Kerberos protocol for distributing the session keys.

[8 marks]

ANSWER:

Table 15.1 Summary of Kerberos Version 4 Message Exchanges

(1)	**C → AS**	$ID_c \| ID_{tgs} \| TS_1$
(2)	**AS → C**	$E(K_c, [K_{c,tgs} \| ID_{tgs} \| TS_2 \| Lifetime_2 \| Ticket_{tgs}])$
		$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_C \| AD_C \| ID_{tgs} \| TS_2 \| Lifetime_2])$

(a) Authentication Service Exchange to obtain ticket-granting ticket

[Ref 1: Pg.488]

Kerberos uses the trusted third party to establish the session keys between each party without compromizing the keys by encrypting session keys using the corresponding parties secret keys.

Index Number | | | | | | | |

(d). List down and briefly describe four (04) deployment models of cloud computing.

[6 marks]

ANSWER: Public cloud: The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud ser- vices. The cloud provider is responsible both for the cloud infrastructure and for the control of data and operations within the cloud.

Private cloud: The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on prem- ise or off premise. The cloud provider (CP) is responsible only for the infra- structure and not for the control.

Community cloud: The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

Hybrid cloud: The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds) [Ref1: Pg 532]

_____ ********** _____